Curriculum Vitae - Hyeonbum Lee

Last update : January 15, 2026

Contact Information

Homepage:hyeonbumlee.github.io
Linkedin:www.linkedin.com/in/hyeonbum-lee
E-mail:hyeonbumlee@snu.ac.kr, leehb3706@gmail.com

Research Background

- **Cryptography**: Zero-Knowledge Proofs, Proof Systems, Secure Multi-Party Computation, Functional Encryption

Current Position

Postdoctoral Researcher Sep 2025 - Present

- Supervisor : Prof. Yongsoo Song
- Institute : Seoul National University, Seoul

Education

Hanyang University, Seoul Mar 2020 - Aug 2025

- Ph.D. Department of Mathematics
- Major: Applied Mathematics (Cryptology)
- Advisor: Prof. Jae Hong Seo.

Hanyang University, Seoul. Mar 2014 - Feb 2018

- B.S. Department of Mathematics

Research Projects

Zero-Knowledge Proofs & Proof Systems

- **A Study on Incremetally Verifiable Computation through Zero-Knowledge Proof**
  Supported by National Security Research Institute (NSR), PI, Sep 2024 - Aug 2025.
- **Logging and Zero-knowledge Proof based on Hierarchical Blockchain, Institute for Information and Communications Technology Promotion**
  Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP), Researcher, May 2022 - Apr 2023.
- **Research on the design technology of a cryptographic proof system suitable for Proof-Carrying Data**
  Supported by National Security Research Institute (NSR), Researcher, Apr 2022 - Oct 2022.
- **A Study on Cryptographic Primitives for SNARK**
  Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP), Research Associate, Apr 2021 - Dec 2026.
- **Research on Incrementally Verifiable Computation Design Technique and Application Method**
  Supported by National Security Research Institute (NSR), Researcher, Apr 2021 - Oct 2021.
- **Research on Post-Quantum Non-Interactive Zero-Knowledge Proofs**
  Supported by National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Feb 2025.
- **Research on Post-Quantum Zero-Knowledge Proofs Design Technique and Application Method**
  Supported by National Security Research Institute (NSR), Researcher, Apr 2020 - Oct 2020.

Others

- **Secure Multi-party Approximate Computation**
  Supported by Samsung Science & Technology Foundation, Researcher, Sep 2021 - Aug 2024.
- **A Study of Functional Encryption and Its Core Techniques**
  Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) & National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Jul 2021.

Selected Publications

Journal

1. Chanyang Ju, **Hyeonbum Lee**, Heewon Chung, Jae Hong Seo, and Sungwook Kim,
   Analysis of Zero-Knowledge Protocols for Verifiable Computation and Its Applications
   Journal of The Korea Institute of Information Security & Cryptology VOL.31, NO.4, Aug. 2020
2. Chanyang Ju, **Hyeonbum Lee**, Heewon Chung, and Jae Hong Seo,
   Efficient Sum-Check Protocol for Convolution
   IEEE Access, VOL.9, pp.164047-164059, 2021, doi
3. Sungwook Kim, **Hyeonbum Lee**, Gwangwoon Lee, and Jae Hong Seo,
   Sublinear Verifier Inner Product Argument under Discrete Logarithm Assumption
   IEEE Transactions on Information Forensics and Security, VOL.18, pp.5332-5344, 2023, doi
4. Changhao Chenli, Wenyi Tang, **Hyeonbum Lee**, and Taeho Jung,
   Fair2Trade: Digital Trading Platform Ensuring Exchange and Distribution Fairness
   IEEE Transactions on Dependable and Secure Computing, VOL.21, pp.4827-4842, 2024, doi
5. **Hyeonbum Lee**, Seunghun Paik, Hyunjung Son, and Jae Hong Seo,
   Cougar: Cubic Root Verifier Inner Product Argument under Discrete Logarithm Assumption
   IEEE Access, Early Access, doi

Conference

1. Sungwook Kim, **Hyeonbum Lee**, Jae Hong Seo, [alphabetical order]
   Efficient Zero-Knowledge Arguments in Discrete Logarithm Setting: Sublogarithmic Proof or Sublinear Verifier
   ASIACRYPT 2022, Taipei, Taiwan, December 5–9, 2022, Proceedings, doi
2. **Hyeonbum Lee**, and Jae Hong Seo,
   TENET *: Sublogarithmic Proof and Sublinear Verifier Inner Product Argument without a Trusted Setup*
   IWSEC 2023, Yokohama, Japan, Aug 29-31, 2023, Proceedings, doi
3. **Hyeonbum Lee**, Kyuhwan Lee, Wenyi Tang, Shankha Shubhra Mukherjee, Jae Hong Seo, and Taeho Jung
   PrivHChain: Monitoring the Supply Chain of Controlled Substances with Privacy-Preserving Hierarchical Blockchain
   Poster Acceptance, IEEE ICBC 2024, Dublin, Ireland, May 27-31, 2024, Proceedings, doi
4. Jaehwan Park, **Hyeonbum Lee**, Junbeom Hur, Jae Hong Seo and Doowon Kim, [co-first author]
   UTRA: Universal Token Reusability Attack and Token Unforgeable Delegatable Order-Revealing Encryption
   ESORICS 2025, Toulouse, France, Sep 22-24, 2025, doi
5. Intak Hwang , **Hyeonbum Lee**, Jinyeong Seo, and Yongsoo Song
   Practical Zero-Knowledge PIOP for Maliciously Secure Multiparty Homomorphic Encryption
   ACM CCS 2025, Taipei, Taiwan, Oct 13-17, 2025, doi

Workshop

1. **Hyeonbum Lee**, and Jae Hong Seo
   On the Security of Nova Recursive Proof System
   6th ZKProof Workshop, Berlin, Germany, May 22-24, 2024, ePrint

Experience

Work Experience

- **Visiting Scholar**
  - Supervisor: Prof. Taeho Jung
    Institute : University of Notre Dame, IN
    Period : Sep 1, 2022 - Mar 1, 2023
- **Teaching Experience**
  - Spring 2025: Mathematical Algorithm, Teaching Fellow (Part-time Lecturer)
  - Spring 2023: PBL: Cryptography, Teaching Fellow (Part-time Lecturer)
  - Spring 2022: Calculus I, Teaching Assistant
  - Spring 2021: Calculus I, Teaching Assistant
  - Fall 2020: Modern Algebra II, Teaching Assistant
  - Spring 2020: Modern Algebra I, Teaching Assistant

Talks & Presentations

Presentations

- *UTRA: Universal Token Reusability Attack and Token Unforgeable Delegatable Order-Revealing Encryption*, Toulouse, Sep 21, 2025
- *How to Design a Zero-Knowledge Proof System in the Discrete Logarithm Setting*
  2024-2 Hanyang Mathematics Colloquium, Seoul, Nov 05, 2024
- *Cougar: Cubic Root Verifier Inner Product Argument under Discrete Logarithm Assumption*
  2024 KMS Annual Meeting, Suwon, Oct 26, 2024
- *On the Security of Nova Recursive Proof System*
  6th ZKProof Workshop, Berlin, May 24, 2024
- *On the Security of Nova IVC*
  2024 KMS Spring Meeting, Daejeon, Apr 19, 2024
- TENET *: Sublogarithmic Proof and Sublinear Verifier Inner Product Argument without a Trusted Setup*
  IWSEC 2023, Yokohama, Aug 30, 2023
- *Efficient Zero-Knowledge Arguments in Discrete Logarithm Setting : Sublogarithmic Proof or Sublinear Verifier*
  Asiacrypt 2022, Taipei, Dec 07, 2022
- *Efficient zero-knowledge arguments in discrete logarithm setting without pairing: Sublinear verifier*
  2022 KMS Spring Meeting, Virtual, Apr 28, 2022
- *Transparent and efficient zero-knowledge arguments from discrete log with better complexity*
  2021 KMS Spring Meeting, Virtual, Apr 30, 2021

Honors & Awards

Awards

- ***Excellence Prize***, National Cryptographic Technology Contest. Oct 2024
  Korea Cryptography Forum
- ***Excellence Prize***, Best Research Paper Award for graduate students Feb 2024
  The Research Institute for Natural Sciences, Hanyang University
- ***Grand Prize***, National Cryptographic Technology Contest. Oct 2022
  Korea Cryptography Forum
- ***Special Prize***, National Cryptographic Technology Contest. Oct 2021, Oct 2023
  Korea Cryptography Forum
- ***SUMMA CUM LAUDE***, Graduate Honors. Feb 2018
  Hanyang University
- ***Dean's list*** 2016 (Fall)
  College of Natural Science, Hanyang University

Scholarships & Stipends

- **Teaching Assistant Scholarship** Sep 2020 - Aug 2022
  Hanyang University
  $6000/year
- **Master and Ph.D Program Scholarship** Mar 2020 - Feb 2023
  Hanyang University
  Full tuition for 3 years (≈ $12000/year)
- **Hanyang Excellent Scientist Scholarship** Mar 2014 - Feb 2018
  Hanyang University
  Full tuition for 4 years (≈ $8000/year)